Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE FACTORIZATION OF THE RATIONAL PRIMES IN A CUBIC DOMAIN.

By G. E. Wahlin.

I. Introduction.

The object of this paper is to determine a set of functions of the coefficients of a cubic equation whose character, with respect to the prime modulus p, completely determines the factorization of p in the cubic domain defined by a root of the equation.

Since every cubic equation can, by a linear transformation, be transformed into the form $x^3 + Cx + D = 0$, where C and D are rational integers, there is no loss in assuming the cubic equation in the following discussion to be of this form. Moreover if $C = p^\lambda \cdot C_1$ and $D = p^\mu \cdot D_1$ where C_1 and D_1 are prime to p, when $\lambda \geqq 2$ and $\mu \geqq 3$ the roots of the equation may be divided by a power of p and the equation thus further reduced. We shall therefore throughout the following pages suppose that $0 \leqq \lambda < 2$ or $0 \leqq \mu < 3$.

We shall denote $x^3 + Cx + D$ by $F_3(x)$ and $3Cx^2 + 9Dx - C^2$ by $F_2(x)$. The discriminant of $F_3(x) = 0$ is $-27D^2 - 4C^3$ and shall be denoted by Δ_3. The discriminant of $F_2(x) = 0$ is $-3\Delta_3$ and shall be denoted by Δ_2.

Let μ_1 and μ_2 be the roots of

$$F_2(x) = 0. \tag{1}$$

Since $F_3(x)$ is supposed to be irreducible $\Delta_3 \neq 0$ and hence $\Delta_2 \neq 0$ and $\mu_1 \neq \mu_2$.

If $\mu_1 = (-9D - \sqrt{\Delta_2})/6C$ and $\mu_2 = (-9D + \sqrt{\Delta_2})/6C$, we shall write $(6C\mu_2)^n = \psi_n(-9D, \Delta_2) + \varphi_n(-9D, \Delta_2)\sqrt{\Delta_2}$ where ψ_n and φ_n are polynomials. Hence $(6C\mu_2)^n - (6C\mu_1)^n = 2\varphi_n(-9D, \Delta_2)\sqrt{\Delta_2}$.

We shall next apply, to the cubic $F_3(x) = 0$, the non-singular transformation

$$x = \frac{\mu_1 y + \mu_2}{y + 1}.$$

After simplifying the new equation has the form $F_3(\mu_1)y^3 + F_3(\mu_2) = 0$. Since

$$F_3(x) = F_2(x)\left(x - \frac{3D}{C}\right) \cdot \frac{1}{3C} - \frac{\Delta_3}{3C^2}x \tag{2}$$

and μ_1 and μ_2 are roots of (1), we have $F_3(\mu_i) = -(\Delta_3/3C^2)\mu_i$ $(i = 1, 2)$

and hence the transformed cubic may be written in the form

$$y^3 + \frac{\mu_2}{\mu_1} = 0 \tag{3}$$

and the roots of this are $\rho^i \sqrt[3]{-(\mu_2/\mu_1)}$ $(i = 0, 1, 2)$, where ρ is a primitive cube root of unity. The roots of $F_3(x) = 0$ are therefore

$$\alpha_i = \frac{\mu_1 \rho^i \sqrt[3]{-\frac{\mu_2}{\mu_1}} + \mu_2}{\rho^i \sqrt[3]{-\frac{\mu_2}{\mu_1}} + 1} \quad (i = 0, 1, 2),$$

and in simplified form $\alpha_0 = -\mu_1^{1/3} \cdot \mu_2^{1/3}(\mu_1^{1/3} + \mu_2^{1/3})$.

The above implies that $C \neq 0$, but this does not invalidate the applications which shall be made of it, because it will be seen that in all cases where it is used C is necessarily different from zero.

The theory underlying the following development is that of the application of the p-adic numbers to the study of the algebraic numbers.*

II. EISENSTEINIAN FUNCTIONS.

A polynomial of the form

$$E(x) = x^n + p^{e_1}a_1x^{n-1} + p^{e_2}a_2x^{n-2} + \cdots + p^{e_{n-1}}a_{n-1}x + p^{e_n}a_n,$$

in which all the coefficients except that of the highest power of x are divisible by the prime p is called an Eisensteinian function. Eisenstein's theorem, that every such polynomial in which $e_n = 1$ is irreducible, is well known. O. Perron† has generalized this theorem as follows. The algebraic equation

$$x^n + p^{[e/n]+1}a_1x^{n-1} + p^{[2e/n]+1}a_2x^{n-2} + \cdots + p^{[(n-1)e/n]+1}a_{n-1}x + p^e a_n = 0,$$

where $a_1, a_2, \cdots a_n$ are arbitrary integers and a_n prime to p and e prime to n is irreducible. The proof of this theorem consists in showing that, in the domain defined by a root of the given equation, p is the nth power of a prime ideal and hence the domain must be of degree n. We note here that this method is also sufficient to show the irreducibility in $k(p)$.

In the "Theorie der Algebraischen Zahlen" Hensel shows that every factor of an Eisensteinian function in $k(p)$ is an Eisensteinian function and hence the number of factors cannot exceed the exponent of p in the last term.

From Perron's theorem we can conclude the following fact:

---

* Hensel, "Theorie der Algebraischen Zahlen." Author, *Transactions Am. Math. Soc.*, Vol. 16. A new development of the theory for quadratic domains was published by Hensel in *Crelle's Journal*, Vol. 144. In the author's paper, here referred to, he gives an extension of this to the general case. Of importance, in the following pages, is the isomorphism between the two domains $k(\mathfrak{p}_i, \alpha)$ and $k(p, \alpha_i^{(r)})$ discussed in the author's paper.

† *Mathematische Annalen*, Vol. 60, Theorem I.

A. If in $E(x)$ $e_i \geqq e_n$, a_n is prime to p and e_n is prime to n, then, in the domain defined by a root of $E(x) = 0$, p is the nth power of a prime divisor and $E(x)$ is irreducible in $k(p)$.

We shall prove the following fact:

B. If in $E(x)$ $e_i \geqq e_{n-1}$, $e_{n-1} \leqq e_n/2$, $n > 2$ and a_{n-1} and a_n are prime to p, then $E(x)$ has a linear factor in $k(p)$.

Since a_{n-1} and a_n are prime to p there exists a c such that $a_{n-1}c + a_n \equiv 0 \bmod p$. Then

$$E(p^{e_n - e_{n-1}}c) = p^{(e_n - e_{n-1})n}c^n + p^{(e_n - e_{n-1})(n-1)+e_1}a_1c^{n-1} + \cdots + p^{(e_n - e_{n-1})2+e_{n-2}}a_{n-2}c^2 + p^{e_n}(a_{n-1}c + a_n).$$

Since $e_{n-1} \leqq e_n/2$, $e_n - e_{n-1} \geqq e_n/2$; and since $n > 2$, $(e_n - e_{n-1})n > e_n$. Since $e_i \geqq e_{n-1}$ for $i \leqq n-2$, $(e_n - e_{n-1})(n-i) + e_i > e_n - e_{n-1} + e_i > e_n$; and since $a_{n-1}c + a_n \equiv 0 \bmod p$, we see that

$$E(p^{e_n - e_{n-1}}c) \equiv 0 \bmod p^{e_n+1}.$$

If we next form $E'(p^{e_n - e_{n-1}}c)$, the first term is divisible by $p^{(e_n - e_{n-1})(n-1)}$ and since $e_n - e_{n-1} \geqq n/2$ and $n - 1 \geqq 2$, it is divisible by p^{e_n}. The following terms up to and including the next to the last are divisible by powers of p whose exponents are, in the successive terms, greater than $e_1, e_2, \cdots e_{n-2}$ and hence greater than e_{n-1}. The last term is divisible only by $p^{e_{n-1}}$. Hence $E(x) = 0$ (p) has a solution in $k(p)$,* and in this domain $E(x) = (x - p^{e_n - e_{n-1}} \cdot \gamma) \cdot Q(x)$.

C. If in B, $e_{n-1} = 1$, $Q(x)$ is seen to be irreducible by Eisenstein's theorem because it is an Eisensteinian function whose last term contains only the first power of p. If in this case $E(x) = 0$ is irreducible in $k(1)$, p is, in the domain defined by a root of this equation, the product of a prime divisor by the $n - 1$th power of another prime, as is seen by A and the isomorphism referred to in the note in the introduction.

We are now ready to consider the factorization of p in the cubic domain $k(\alpha_i)$. I shall denote the prime divisors by $\mathfrak{p}$. As there is no danger of any ambiguity regarding the degrees of the various prime divisors, I shall make no indications of them in the statement of results.

We shall first consider the case when $p > 3$ and is not a divisor of Δ_3.

III. Δ_2 A QUADRATIC RESIDUE MOD p.

Since $\Delta_2 = 81D^2 + 12C^3$ it may happen in this case that $C \equiv 0 \bmod p$ and we shall consider this possibility first.

Since p is not a factor of Δ_3 it is not a factor of the discriminant of $k(\alpha_i)$ and is therefore not divisible by a power of a prime divisor. Moreover the number of factors of $F_3(x)$ in $k(p)$ is the same as the number of factors of $F_3(x)$ mod p.[*] When $C \equiv 0$ mod p, $F_3(x) \equiv x^3 + D$ mod p and we see that when $p \equiv 1$ mod 3, if $-D$ is a cubic residue mod p, $F_3(x) \equiv 0$ mod p has three solutions in $k(1)$, and when $-D$ is not a cubic residue the same congruence has no rational solution. If $p \equiv -1$, $-D$ is always a cubic residue mod p but in this case $F_3(x) \equiv 0$ mod p has only one solution in $k(1)$. Hence when $p \equiv +1$ mod 3, if $-D$ is a cubic residue mod p, $F_3(x)$ is in $k(p)$ the product of three linear factors, if $-D$ is not a cubic residue mod p, $F_3(x)$ is irreducible in $k(p)$ and when $p \equiv -1$ mod 3, $F_3(x)$ is the product of a linear and a quadratic factor in $k(p)$.

---

* Hensel, A.Z., p. 71, bottom.

Since the cubic character of $-D$ is the same as the cubic character of Δ_3 we can conclude that, when $p \equiv +1$ mod 3 if $\Delta_3^{(p-1)/3} \equiv 1$ mod p, then $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$, and if $\Delta_3^{(p-1)/3} \not\equiv 1$ mod p, then $p \sim \mathfrak{p}$; and when $p \equiv -1$ mod 3, then $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$.

If $C \not\equiv 0$ mod p the roots of (1) are units with respect to p. Since Δ_2 is a quadratic residue $F_2(x)$ is reducible in $k(p)$. Hence, if Δ_2 is not a square, $p \sim \mathfrak{p}' \cdot \mathfrak{p}''$ in $k(\mu_1)$ and if Δ_2 is a square, $k(\mu_1) = k(1)$ and $p \sim \mathfrak{p}'$.

Let us now consider the equation

$$y^3 + \frac{\mu_2}{\mu_1} = 0 \qquad (\mathfrak{p}'). \tag{4}$$

If $p \equiv -1$ mod 3 this will always have a solution in $k(\mathfrak{p}', \mu_1)$ but if $p \equiv 1$ mod 3 it has a solution when and only when $(\mu_2/\mu_1)^{(n-1)/3} \equiv 1$ mod $\mathfrak{p}'$. But this condition is equivalent to $\mu_2^{(p-1)/3} - \mu_1^{(p-1)/3} \equiv 0$ mod $\mathfrak{p}'$ and hence according to the notation in the introduction it is seen to be equivalent to $\varphi_{(p-1)/3}(-9D, \Delta_2) \equiv 0$ mod $\mathfrak{p}'$. But $\varphi_{(p-1)/3}(-9D, \Delta_2)$ is a rational integer and is therefore divisible by $\mathfrak{p}'$ when and only when it is divisible by p. Hence in order that (4) shall have a solution in $k(\mathfrak{p}', \mu_1)$ it is necessary and sufficient, either that $p \equiv -1$ mod 3, or that $\varphi_{(p-1)/3}(-9D, \Delta_2) \equiv 0$ mod p.

Every number of $k(\mathfrak{p}', \mu_1)$ is for the domain of $\mathfrak{p}'$ equal to a number of $k(p)$ and hence there exist rational p-adic numbers m_1 and m_2 such that $\mu_1 = m_1$ $(\mathfrak{p}')$ and $\mu_2 = m_2$ $(\mathfrak{p}')$ and if (4) has a solution this is also for the domain of $\mathfrak{p}'$ equal to a rational p-adic number b.

Let $\overline{\mathfrak{p}}'$ be that prime divisor of $\mathfrak{p}'$ in $k[\mu_1, \sqrt[3]{-(\mu_2/\mu_1)}]$ corresponding to the linear factor of (4). Then $\sqrt[3]{-(\mu_2/\mu_1)} = b$ $(\overline{\mathfrak{p}}')$ and $\overline{\mathfrak{p}}'$ being a factor of $\mathfrak{p}'$, $\mu_1 = m_1$ and $\mu_2 = m_2$ $(\overline{\mathfrak{p}}')$. Hence, if we put $a_0 = (m_1 b + m_2)/(b + 1)$ we see that $\alpha_0 = a_0$ $(\overline{\mathfrak{p}}')$ and hence $F_3(a_0) = 0$ $(\overline{\mathfrak{p}}')$. But from this it follows that $F_3(x) = (x - a_0)Q(x)$ $(\overline{\mathfrak{p}}')$, and since the coefficients of both members of this equation are rational p-adic numbers it is evident that the two members are equal for the domain of $\overline{\mathfrak{p}}'$ when and only when they are equal for the domain of p, and hence

---

[*] Hensel, A.Z., p. 68.

$$F_3(x) = (x - a_0)\cdot Q(x) \quad (p) \tag{5}$$

if (4) has a solution in $k(\mathfrak{p}', \mu_1)$.

If however (4) does not have a solution in $k(\mathfrak{p}', \mu_1)$, it is irreducible in this domain and the same is then also true of $F_3(x)$ and hence a fortiori it is irreducible in $k(p)$.

In regard to $Q(x)$ we observe that since its discriminant differs from Δ_3 only by a square factor it is reducible when Δ_3 is a quadratic residue mod p and is irreducible when Δ_3 is not a quadratic residue mod p. But $\Delta_2 = -3\Delta_3$ is a quadratic residue mod p and hence Δ_3 is a quadratic residue when and only when -3 is a quadratic residue and hence when and only when $p \equiv 1 \bmod 3$.

Hence when $p \equiv 1 \bmod 3$ if $\varphi_{(p-1)/3}(-9D, \Delta_2) \equiv 0 \bmod p$, then $F_3(x)$ is in $k(p)$ the product of three linear factors and if $\varphi_{(p-1)/3}(-9D, \Delta_2) \not\equiv 0 \bmod p$, $F_3(x)$ is irreducible in $k(p)$; and when $p \equiv -1 \bmod 3$, $F_3(x)$ is in $k(p)$ the product of a linear and a quadratic factor.

Regarding the factors of p in $k(\alpha_i)$ we can conclude that when $p \equiv 1 \bmod 3$ and $\varphi_{(p-1)/3}(-9D, \Delta_2) \equiv 0 \bmod p$, then $p \sim \mathfrak{p}_1\cdot\mathfrak{p}_2\cdot\mathfrak{p}_3$; when $p \equiv 1 \bmod 3$ and $\varphi_{(p-1)/3}(-9D, \Delta_2) \not\equiv 0 \bmod p$, then $p \sim \mathfrak{p}$; and when $p \equiv -1 \bmod 3$, then $p \sim \mathfrak{p}_1\cdot\mathfrak{p}_2$.

IV. Δ_2 NOT A QUADRATIC RESIDUE MOD p.

When Δ_2 is not a quadratic residue mod p, $F_2(x)$ is irreducible in $k(p)$ and hence in $k(\mu_1)$ p is a prime of the second degree. Using the same method as in III we see that the equation

$$y^3 + \mu_2/\mu_1 = 0 \qquad (p) \tag{6}$$

has a solution in $k(p, \mu_1)$ when and only when $\varphi_{(p^2-1)/3}(-9D, \Delta_2) \equiv 0 \bmod p$ because in this case it is necessary and sufficient that $(\mu_2/\mu_1)^{(p^2-1)/3} \equiv 1 \bmod p$.

Let us suppose that a solution exists and that $\bar{\mathfrak{p}}$ is the prime divisor of p in $k[\mu_1\sqrt[3]{-(\mu_2/\mu_1)}]$ corresponding to the linear factor of (6). Then there exists an a_0 in $k(p, \mu_1)$ such that $\alpha_0 = a_0(\bar{\mathfrak{p}})$ and hence as above $F_3(x) = (x - a_0)Q(x)$ $(\bar{\mathfrak{p}})$. Again since the coefficients of both members of this equation belong to $k(p, \mu_1)$ in which p is a prime, we see that it is true for the domain of $\bar{\mathfrak{p}}$ when and only when it is true for the domain of p. Hence

$$F_3(x) = (x - a_0)\bar{Q}(x) \quad (p). \tag{7}$$

If a_0 is a rational number, $F_3(x)$ has a linear factor in $k(p)$. If a_0 is a quadratic number and a_0' its conjugate since $F_3(a_0) = 0$ (p), we know that $F_3(a_0') = 0$ (p). Hence $F_3(x) = (x - a_0)\cdot(x - a_0')(x - a)$ (p) and since the coefficients of $(x - a_0)(x - a_0')$ are rational a must be rational and again we see that $F_3(x)$ has a linear factor in $k(p)$.

If (6) has no solution in $k(p, \mu_1)$ in the same way as in III, we conclude that $F_3(x)$ is irreducible in $k(p)$.

Considering the case when $F_3(x)$ is reducible let us write $F_3(x) = (x - a)\cdot Q(x)$. As in III we conclude that $Q(x)$ is reducible when and only when Δ_3 is a quadratic residue mod p and since now Δ_2 is not a quadratic residue this is the case when and only when -3 is not a quadratic residue and hence $p \equiv -1 \bmod 3$.

Hence when $\varphi_{(p^2-1)/3}(-9D, \Delta_2) \equiv 0 \bmod p$ and $p \equiv -1 \bmod 3$, $p \sim \mathfrak{p}_1\cdot\mathfrak{p}_2\cdot\mathfrak{p}_3$; when $\varphi_{(p^2-1)/3}(-9D, \Delta_2) \equiv 0 \bmod p$ and $p \equiv 1 \bmod 3$, $p \sim \mathfrak{p}_1\cdot\mathfrak{p}_2$; and when $\varphi_{(p^2-1)/3}(-9D, \Delta_2) \not\equiv 0 \bmod p$, $p \sim \mathfrak{p}$.

V. $\Delta_2 \equiv 0$ MOD p, $p > 3$.

We shall next consider the factorization of those primes which are greater than 3 and are factors of the discriminant of $F_3(x)$. We shall write $\Delta_3 = p^s\Delta_3'$ where we suppose that Δ_3' is prime to p. As stated in I we shall put $C = p^\lambda\cdot C_1$, and $D = p^\mu D_1$. Since $s > 0$ if λ or μ is zero the other must be zero also and we shall consider this possibility first. From (2) we have

$$F_3(x) \equiv F_2(x)\cdot\left(x - \frac{3D}{C}\right)\cdot\frac{1}{3C} \bmod p^s \tag{8}$$

and the resultant of the two factors $R = R[F_2(x),\ x - (3D/C)] = 1/C\cdot(54D^2 - C^3)$. Since $\Delta_3 = 27D^2 + 4C^3 \equiv 0 \bmod p$, $27D^2 \equiv -4C^3 \bmod p$ and hence $R \equiv -9C^2 \bmod p$ and is therefore prime to p. Hence $F_3(x)$ is reducible in $k(p)$.*

We shall again write $F_3(x) = (x - a)Q(x)\ (p)$ and studying the quadratic factor in the same way as in III we can conclude that when s is even and Δ_3' is a quadratic residue, $Q(x)$ is reducible in $k(p)$, and when s is even and Δ_3' is not a quadratic residue mod p, it is irreducible.

Using the isomorphism mentioned in the note in I we can conclude that when s is even if Δ_3' is a quadratic residue mod p, then $p \sim \mathfrak{p}_1\cdot\mathfrak{p}_2\cdot\mathfrak{p}_3$ in $k(\alpha_i)$ and when Δ_3' is not a quadratic residue mod p, then $p \sim \mathfrak{p}_1\cdot\mathfrak{p}_2$ in $k(\alpha_i)$. When s is odd, $p \sim \mathfrak{p}_1\cdot\mathfrak{p}_2^2$ in $k(\alpha_i)$.

If however $\lambda > 0$ it follows that $\mu > 0$ and we need only consider the cases when $\lambda < 2$ or $\mu < 3$. We shall take up the two cases (*a*) $\lambda \geqq \mu$ and (*b*) $\lambda < \mu$.

(*a*) Since $\lambda \geqq \mu > 0$ by the restrictions imposed on λ and μ we conclude that in this case $\mu = 1$ or 2 and hence by II, *A* we know that $F_3(x)$ is irreducible in $k(p)$ and $p \sim \mathfrak{p}^3$ in $k(\alpha_i)$.

---

* Hensel, A.Z., p. 71.

(*b*) Since now $\lambda < \mu$ we see that this is possible only when $\lambda = 1$ and hence, by II, B and C, we can conclude that $F_3(x)$ is in $k(p)$ the product of a linear and a quadratic factor and $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$ in $k(\alpha_i)$.

VI. $p = 3$.

We shall next consider the factorization of 3 in $k(\alpha_i)$. As before we shall write $C = 3^\lambda C_1$, $D = 3^\mu D_1$ and $\Delta_3 = 3^s \Delta_3'$. If $\lambda = 0$, $s = 0$ and we need only consider $F_3(x)$ with respect to the modulus 3. There are six possible forms as follows:

$F_3(x) \equiv x^3 + x \equiv x(x^2 + 1)$; $\Delta_3 \equiv -1 \bmod 3$,
$F_3(x) \equiv x^3 + 2x \equiv x(x-1)(x+1)$; $\Delta_3 \equiv 1 \bmod 3$,
$F_3(x) \equiv x^3 + x + 1 \equiv (x-1)(x^2 + x + 2)$; $\Delta_3 \equiv -1 \bmod 3$,
$F_3(x) \equiv x^3 + 2x + 1$ irreducible; $\Delta_3 \equiv 1 \bmod 3$,
$F_3(x) \equiv x^3 + x + 2 \equiv (x-2)(x^2 + 2x + 2)$; $\Delta_3 \equiv -1 \bmod 3$,
$F_3(x) \equiv x^3 + 2x + 2$ irreducible; $\Delta_3 \equiv 1 \bmod 3$.

From a consideration of this table we note that when $\Delta_3 \equiv 1 \bmod 3$, $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ if $D \equiv 0 \bmod 3$ and $3 \sim \mathfrak{p}$ if $D \not\equiv 0 \bmod 3$; and when $\Delta_3 \equiv -1 \bmod 3$, then $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$.

If $s > 0$ it is necessary that $\lambda > 0$. As before we need only consider the cases when $\lambda < 2$ or $\mu < 3$. These we shall consider as follows (*a*) $\lambda = 1$, $\mu = 0$; (*b*) $\lambda > 1$, $\mu = 0$; (*c*) $\lambda \geqq \mu$; (*d*) $\lambda < \mu$.

(*a*) When $\lambda = 1$, $\mu = 0$, $\Delta_3 = -27(D^2 + 4C_1^3)$ and $s \geqq 3$. The function $F_2(x)$ is $9C_1x^2 + 9Dx - 9C_1^2$ and μ_1 and μ_2 are roots of

$$C_1x^2 + Dx - C_1^2 = 0. \tag{9}$$

In place of the equation (2) we have now

$$F_3(x) = (C_1x^2 + Dx - C_1^2)\left(x - \frac{D}{C_1}\right) \cdot \frac{1}{C_1} - \frac{\Delta_3}{27C_1}x \tag{10}$$

and hence when $s > 3$,

$$F_3(x) \equiv (C_1x^2 + Dx - C_1^2)\left(x - \frac{D}{C_1}\right) \cdot \frac{1}{C_1} \bmod 3^{s-3}. \tag{11}$$

Since in this case (i.e., $s > 3$) $D^2 + 4C_1^3 \equiv 0 \bmod 3^{s-3}$,

$$D^2 \equiv -4C_1^3 \bmod 3^{s-3}. \tag{12}$$

Therefore

$$F_3'\left(\frac{D}{C_1}\right) \quad \frac{3D^2 + 3C_1^3}{C_1^2} = \frac{3}{C_1^2}(D^2 + C_1^3) \equiv -9C_1 \bmod 3^{s-3}$$

and if $s > 6$, $F_3'(D/C_1)$ is divisible only by 3^2. $F_3''(D/C_1)/2! = 3(D/C_1)$ and is divisible only by 3. $F_3'''(D/C_1)/3! = 1$ and is prime to 3. Hence using the theorem on pages 73 and 74 of Hensel's Theorie der Algebraischen

Zahlen we see that when $s > 6$, $F_3(x)$ has a linear factor in $k(3)$, and shall write

$$F_3(x) = (x - a)Q(x) \cdot (3).$$

Regarding the quadratic factor we can conclude in the same way as in V that it is reducible when and only when s is even and $\Delta'_3 \equiv 1 \bmod 3$. By the isomorphism previously used we then see that if s is even, when $\Delta'_3 \equiv 1 \bmod 3$, $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$, and when $\Delta'_3 \equiv -1 \bmod 3$, $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$; and that when s is odd, $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$.

If $s = 6$, let us consider first the case when Δ'_3 is not a quadratic residue mod 3. Then

$$\Delta^t_3 = -\frac{D^2 + 4C_1^3}{27} \equiv -1 \bmod 3 \tag{13}$$

and since $D^2 + 4C_1^3 \equiv 0 \bmod 3$ and $D^2 \equiv 4 \equiv 1 \bmod 3$, $C^3 \equiv -1 \bmod 3$ and we can write (13) in the form

$$-\frac{D^2 + 4C_1^3}{27} \equiv C_1^3 \bmod 3$$

whence $-D^2 - 4C_1^3 \equiv 27C_1^3 \bmod 81$ or

$$D^2 \equiv -31C_1^3 \bmod 81. \tag{14}$$

Now

$$F_3\left(-\frac{2D}{C_1}\right) = -\frac{D}{C_1^3}(8D^2 + 5C_1^3) \equiv 243D \equiv 0 \bmod 81$$

by (14).

$$F'_3\left(-\frac{2D}{C_1}\right) = \frac{3}{C_1^2}(4D^2 + C_1^3) \equiv -123 \cdot 3C_1 \bmod 81,$$

and is therefore divisible only by 3^2.

$$F''_3\left(-\frac{2D}{C_1}\right)\Big/2! = -\frac{6D}{C_1}$$

and is divisible only by 3.

$$F'''_3\left(-\frac{2D}{C_1}\right)\Big/3! = 1$$

and is prime to 3. In the same way as above we can conclude that $F_3(x)$ has a linear factor in $k(3)$ and since Δ'_3 is not a quadratic residue the quadratic factor is irreducible in $k(3)$ and as above we conclude that $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$ in $k(\alpha_i)$.

If however $s = 6$ and Δ'_3 is a quadratic residue mod 3, (10) shows that $F_3(D/C_1)$ is divisible by 3^3 but not by 3^4. Since now

$$\Delta'_3 = -\frac{D^2 + 4C_1^3}{27} \equiv 1 \equiv -C_1^3 \bmod 3,$$

$-D^2 - 4C_1^3 \equiv -27C_1^3 \bmod 81$ and

$$D^2 \equiv 23C_1^3 \bmod 81. \tag{15}$$

Let us now form

$$F_3\left(3y + \frac{D}{C_1}\right) = 27y^3 + 27\frac{D}{C_1}y^2 + 9\left(\frac{D^2}{C_1^2} + C_1\right)y + F_3\left(\frac{D}{C_1}\right).$$

Dividing by 27 and equating to zero we have

$$y^3 + \frac{D}{C_1}y^2 + \frac{D^2 + C_1^3}{3C_1^2}y + F_3\left(\frac{D}{C_1}\right)\Big/27 = 0 \tag{16}$$

and evidently one root of this equation belongs to $k(\alpha_i)$. In this equation D/C_1 and $F_3(D/C_1)/27$ are known to be prime to 3. By (15) $D^2 + C_1^3 \equiv 24C_1^3 \bmod 81$ and hence $(D^2 + C_1^3)3C_1^2 \equiv 8C_1 \bmod 27$ and is therefore also prime to 3.

We shall next see that the left-hand member of (16) is irreducible mod 3. Suppose that it is not. It must then have a linear factor and hence there must exist an a such that

$$a^3 + \frac{D}{C_1}a^2 + \frac{D^2 + C_1^3}{3C_1^2}a + F_3\left(\frac{D}{C_1}\right)\Big/27 \equiv 0 \bmod 3.$$

Since the last term is prime to 3, a cannot be divisible by 3 and hence $a^3 \equiv a \bmod 3$ and $a^2 \equiv 1 \bmod 3$ and a must satisfy

$$\left(1 + \frac{D^2 + C_1^3}{3C_1^2}\right)a + \frac{D}{C_1} + F_3\left(\frac{D}{C_1}\right)\Big/27 \equiv 0 \bmod 3. \tag{17}$$

We have seen that $(D^2 + C_1^3)/3C_1^2 \equiv 8C_1 \bmod 27$ and since $C_1^3 \equiv -1 \bmod 3$, $C_1 \equiv -1 \bmod 3$ and hence $(D^2 + C_1^3)/3C_1^2 \equiv -8 \equiv 1 \bmod 3$.

$$\frac{D}{C_1} + F_3\left(\frac{D}{C_1}\right)\Big/27 = \frac{D}{27C_1^3}[27C_1^2 + D^2 + 4C_1^3].$$

By 15 we have $27C_1^2 + D^2 + 4C_1^3 \equiv 27C_1^2 + 27C_1^3 \bmod 81$ and hence

$$\frac{D}{27C_1^3}[27C_1^2 + D^2 + 4C_1^3] \equiv \frac{D}{C_1}(1 + C_1) \equiv 0 \bmod 3.$$

The congruence (17) therefore reduces to $2a \equiv 0 \bmod 3$ which is impossible since a is prime to 3. The left-hand member of (16) is therefore irreducible mod 3 and hence also in $k(3)$. Since this is so we know that 3 cannot be a divisor of the discriminant of (16) and hence also not a divisor of the discriminant of $k(\alpha_i)$ and is therefore not divisible by a power of a prime divisor and hence $3 \sim \mathfrak{p}$ in $k(\alpha_i)$.

If $s = 5$, $F_3(D/C_1)$ is divisible by 9 but not by 27. Multiplying (16) by 3 and forming the equation whose roots are the reciprocals of the roots of (16) we have

$$\frac{F_3(D/C_1)}{9} z^3 + \frac{D^2 + C_1^3}{C_1^2} z^2 + \frac{3D}{C_1} z + 3 = 0$$

and by II, *A* we see that this is irreducible in $k(p)$ and that in $k(\alpha_i)$ $3 \sim \mathfrak{p}^3$.

If $s = 4$, $F_3(D/C_1)$ is divisible only by 3 and hence the equation

$$F\left[y + \left(\frac{D}{C_1}\right)\right] = 0$$

is seen by II, *A* to be irreducible in $k(3)$ and again $3 \sim \mathfrak{p}^3$ in $k(\alpha_i)$.

If $s = 3$, $\Delta'_3 = -D^2 - 4C_1^3$ and the discriminant of (9) is $-\Delta'_3$ Since $D^2 \equiv 1 \bmod 3$ and $\Delta'_3 \not\equiv 0 \bmod 3$ it is necessary that $C \equiv 1 \bmod 3$ and hence $-\Delta'_3 \equiv 2 \bmod 3$. The equation (9) is therefore irreducible in $k(3)$ and in $k(\mu_1)$ 3 is a prime of the second degree. As in IV we can show that $F_3(x)$ is reducible in $k(3)$ when and only when the equation $y^3 + (\mu_2/\mu_1) = 0$ (3) has a solution in $k(3, \mu_1)$. This equation has a solution when and only when the congruence $y^3 + (\mu_2/\mu_1) \equiv 0 \bmod 9$ has a solution in the given domain.*

If the given congruence has a solution b, we see that $b^9 \equiv -(\mu_2/\mu_1)^3 \bmod 27$ and since every integer of $k(3, \mu_1)$ satisfies the congruence $x^9 \equiv x \bmod 3$, we conclude that $b \equiv -(\mu_2/\mu_1)^3 \bmod 3$. Hence if $y^3 + (\mu_2/\mu_1) \equiv 0 \bmod 9$ has a solution, there must exist a c such that $[3c - (\mu_2/\mu_1)^3]^3 + \mu_2/\mu_1 \equiv 0 \bmod 9$. By expanding we find that the necessary and sufficient condition for the reducibility of $F_3(x)$ is $-(\mu_2/\mu_1)^9 + \mu_2/\mu_1 \equiv 0 \bmod 9$, or $(\mu_2/\mu_1)^8 \equiv 1 \bmod 9$ which reduces to $\varphi_8(-D, -\Delta'_3) \equiv 0 \bmod 9$.

But $\varphi_8(-D, -\Delta'_3) = -8D^7 + 56D^5\Delta'_3 - 56D^3\Delta'^2_3 + 8D\Delta'^3_3$ and hence since $8D$ is relatively prime to 3, the necessary and sufficient condition is $\Delta'^3_3 - 7\Delta'^2_3 D^2 + 7\Delta'_3 D^4 - D^6 \equiv 0 \bmod 9$ or in another form

$$\left(\frac{\Delta'_3}{D^2}\right)^3 - 7\left(\frac{\Delta'_3}{D^2}\right)^2 + 7\left(\frac{\Delta'_3}{D^2}\right) - 1 \equiv 0 \bmod 9. \tag{18}$$

But 1 is the only rational solution of $x^3 - 7x^2 + 7x - 1 \equiv 0 \bmod 9$ and hence (18) is possible when and only when $\Delta'_3/D^2 \equiv 1 \bmod 9$, or $-D^2 - 4C_1^3 \equiv D^2 \bmod 9$. This reduces to $D^2 + 2C_1^3 \equiv 0 \bmod 9$ and since $C_1 \equiv 1 \bmod 3$, $C_1^3 \equiv 1 \bmod 9$ and hence this condition is equivalent to $D^2 + 2 \equiv 0 \bmod 9$.

Hence $F_3(x)$ is reducible in $k(3)$ when and only when $D^2 + 2 \equiv 0 \bmod 9$. Since $s = 3$, 3 is in $k(\alpha_i)$ divisible by a power of a prime divisor and hence $F_3(x)$ cannot have three linear factors in $k(3)$. We can therefore conclude that when $D^2 + 2 \equiv 0 \bmod 9$, $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$, and when $D^2 + 2 \not\equiv 0 \bmod 9$, $s \sim \mathfrak{p}^3$.

---

* Author, *Crelle's Journal*, Vol. 145.

(*b*) Since in this case $\lambda > 1$, $\mu = 0$, we have $s = 3$ and again $F_3(x)$ is either irreducible or the product of a linear and a quadratic factor in $k(3)$. If $D^2 \equiv 1 \bmod 9$, $F_3(-D) \equiv 0 \bmod 9$ and hence $F_3(x-D)$ is by II, *B* seen to be reducible and hence $F_3(x)$ is in $k(3)$ the product of a linear and a quadratic factor. If $D^2 \not\equiv 1 \bmod 9$, $F_3(-D)$ is divisible by 3 but not by 9 and hence by II, *A*, $F_3(x-D)$ is seen to be irreducible in $k(3)$.

Hence when $D^2 \equiv 1 \bmod 9$, $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$ and when $D^2 \not\equiv 1 \bmod 9$, $3 \sim \mathfrak{p}^3$.

(*c*) In this case $\lambda \geqq \mu > 0$ and hence by the restrictions imposed on λ and μ we conclude that $\mu = 1$ or 2 and by II, *A*, $F_3(x)$ is irreducible in $k(3)$ and in $k(\alpha_i)$, $3 \sim \mathfrak{p}^3$.

(*d*) In this case $\lambda < \mu$ and again by the restrictions on λ and μ we see that this is possible only when $\lambda = 1$ and by II, *B* we conclude that $F_3(x)$ is in $k(3)$ the product of a linear and a quadratic factor and in $k(\alpha_i)$, $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$.

VII. $p = 2$.

We observe that when $p = 2$ if D is odd $s = 0$ and Δ_3 is not divisible by 2 and we need only consider $F_3(x)$ relative to the modulus 2. Two possibilities occur as follows:

$$F_3(x) \equiv x^3 + x + 1 \text{ irreducible mod } 2,$$
$$F_3(x) \equiv x^3 + 1 \equiv (x-1)(x^2 + x + 1) \bmod 2.$$

Hence when C is odd, $F_3(x)$ is irreducible in $k(2)$ and in $k(\alpha_i)$, $2 \sim \mathfrak{p}$; and when C is even, $F_3(x)$ is in $k(2)$ the product of a linear and a quadratic factor in $k(2)$ and in $k(\alpha_i)$, $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$.

If $s > 0$ it is necessary that $\mu > 0$ and we shall consider the cases (*a*) $\lambda = 0$, $\mu \geqq 1$; (*b*) $\lambda \geqq \mu$; (*c*) $\lambda < \mu$.

(*a*) In this case $s \geqq 2$. We have $F_3(x) \equiv x(x^2 + C) \bmod 2^\mu$ and since $R(x, x^2 + C) = C$ is odd we conclude that in this case $F_3(x)$ has a factor in $k(2)$* and we shall write $F_3(x) = (x-a)Q(x)$. Using the same reasoning as before we see that when s is even and $\Delta_3' \equiv 1 \bmod 8$, then the quadratic factor is reducible and, in all other cases, irreducible.

We can then conclude by making use of the isomorphism previously referred to and the factorization of 2 in a quadratic domain† that when s is even, if $\Delta_3' \equiv 1 \bmod 8$, then $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$, and if $\Delta_3' \not\equiv 1 \bmod 8$ but $\Delta_3' \equiv 1 \bmod 4$, then $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$, and if $\Delta_3' \equiv 3 \bmod 4$ or when s is odd, $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$.

(*b*) Since in this case $\lambda \geqq \mu$ as in IV, (*c*), we can conclude that $\mu = 1$ or 2 and by II, *A*, $F_3(x)$ is irreducible in $k(2)$ and $2 \sim \mathfrak{p}^3$ in $k(\alpha_i)$.

(*c*) Since in this case $\lambda < \mu$ we know again that $\lambda = 1$ and again by II, *B* and *C*, $F_3(x)$ is in $k(2)$ the product of a linear and a quadratic factor and in $k(\alpha_i)$, $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$.

---

* Hensel, A.Z., p. 71.

† Hilbert, Report, *Jahresbericht der Deut. Math. ver.*, Vol. 4.

SUMMARY.

$p > 3$

$\Delta_2{}^{(p-1)/2} \equiv 1 \bmod p$

$p \equiv 1 \bmod 3$

$$\left.\begin{array}{ll} C \equiv 0 \bmod p, & \Delta_3^{(p-1)/3} \equiv 1 \bmod p \\ C \not\equiv 0 \bmod p, & \varphi_{(p-1)/3}(-9D, \Delta_2) \equiv 0 \bmod p \end{array}\right\} p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$$

$$\left.\begin{array}{ll} C \equiv 0 \bmod p, & \Delta_3^{(p-1)/3} \not\equiv 1 \bmod p \\ C \not\equiv 0 \bmod p, & \varphi_{(p-1)/3}(-9D, \Delta_2) \not\equiv 0 \bmod p \end{array}\right\} p \sim \mathfrak{p}$$

$p \equiv -1 \bmod 3$ . . . . $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$

$\Delta_2{}^{(p-1)/2} \equiv -1 \bmod p$

$\varphi_{(p^2-1)/3}(-9D, \Delta_2) \equiv 0 \bmod p$

$p \equiv -1 \bmod 3$ . . . . $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$

$p \equiv 1 \bmod 3$ . . . . $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$

$\varphi_{(p^2-1)/3}(-9D, \Delta_2) \not\equiv 0 \bmod p$ . . . . $p \sim \mathfrak{p}$

$\Delta_2 \equiv 0 \bmod p, \quad \Delta_3 = p^s \Delta'_3$

$\lambda = \mu = 0$

s even

$(\Delta'_3)^{(p-1)/2} \equiv 1 \bmod p$ . . . . $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$

$(\Delta'_3)^{(p-1)/2} \equiv -1 \bmod p$ . . . . $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$

s odd . . . . $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$

$\lambda \geqq \mu > 0$ . . . . $p \sim \mathfrak{p}^3$

$0 < \lambda < \mu$ . . . . $p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$

$p = 3$

$\lambda = 0$

$\Delta_3 \equiv 1 \bmod 3$

$D \equiv 0 \bmod 3$ . . . . $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$

$D \not\equiv 0 \bmod 3$ . . . . $3 \sim \mathfrak{p}$

$\Delta_3 \equiv 2 \bmod 3$ . . . . $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$

$\lambda = 1, \quad \mu = 0$

$s \geqq 7$

s even

$\Delta'_3 \equiv 1 \bmod 3$ . . . . $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$

$\Delta'_3 \equiv -1 \bmod 3$ . . . . $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$

s odd . . . . $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$

$s = 6$

$\Delta'_3 \equiv 1 \bmod 3$ . . . . $3 \sim \mathfrak{p}$

$\Delta'_3 \equiv -1 \bmod 3$ . . . . $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$

$s = 5$ or 4 . . . . $3 \sim \mathfrak{p}^3$

$s = 3$

$D^2 + 2 \equiv 0 \bmod 9$ . . . . $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$

$D^2 + 2 \not\equiv 0 \bmod 9$ . . . . $3 \sim \mathfrak{p}^3$

- $\lambda > 1, \quad \mu = 0$
    - $D^2 \equiv 1 \bmod 9$ …… $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$
    - $D^2 \not\equiv 1 \bmod 9$ …… $3 \sim \mathfrak{p}^3$
- $\lambda \geqq \mu > 0$ …… $3 \sim \mathfrak{p}^3$
- $\lambda < \mu$ …… $3 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$

$p = 2$

- $\mu = 0$
    - $C \equiv 0 \bmod 2$ …… $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$
    - $C \not\equiv 0 \bmod 2$ …… $2 \sim \mathfrak{p}$
- $\lambda = 0, \quad \mu \geqq 1$
    - s even
        - $\Delta_3' \equiv 1 \bmod 8$ …… $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$
        - $\Delta_3' \not\equiv 1 \bmod 8$
            - $\Delta_3' \equiv 1 \bmod 4$ …… $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2$
            - $\Delta_3' \equiv 3 \bmod 4$ …… $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$
    - s odd …… $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$
- $\lambda \geqq \mu > 0$ …… $2 \sim \mathfrak{p}^3$
- $\lambda < \mu$ …… $2 \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$